MARYLAND DEPARTMENT OF JUVENILE SERVICES

POLICY & PROCEDURE

SUBJECT: **Firewall Security Policy**
NUMBER: **IT-01-08 (Information Technology)**
APPLICABLE TO: **DJS Information Technology Unit**
EFFECTIVE DATE: **June 6, 2008**

Approved: "/s/signature on original copy"
Donald W. DeVore, Secretary

1. **POLICY.** The Department of Juvenile Services (DJS) establishes this policy to provide guidelines for the configuration and administration of the DJS Information Technology Firewall. DJS is committed to ensuring the Department's information technology security program is in compliance with State security policies and standards, and State and federal laws and regulations.

2. **AUTHORITY.**

a. State of Maryland Department of Budget and Management - *Information Technology Security Policy and Standards* – Version 1.5 (January, 2007) - Sections 7.3 and 7.4.
b. National Institute of Standards and Technology Special Publication 800-41 - *Guidelines on Firewalls and Firewall Policy - Section C.5.*

3. **DEFINITIONS.**

a. *Chief Information Officer (CIO)* means the individual responsible for managing the Information Technology Unit.
b. *Data Security Officer* means the individual responsible for ensuring the Information Technology Unit is in compliance with the security guidelines established by Department of Budget and Management (DBM).
c. *Demilitarized Zone* means separate interface in the firewall to protect the internal network from external intrusions.
d. *Firewall* means a network device which provides protection for the network against unauthorized access, intrusions and security breaches.
e. *Firewall Administrator* means the individual responsible for managing the activities of the firewall.
f. *Information Technology* Unit (IT) means individuals responsible for DJS network, applications, telecommunication and technical support.
g. Intrusion Detection/Prevention (IDP) means a device that detects attacks and other security violations, and detects and deals with the preambles to attacks.
h. *Network* means a system containing any combination of computers, servers, printers, audio and visual display devices, or telephones inter-connected by cables and telecommunication devices to transfer and receive information.

i. *Patch* means software used to fix or update applications and operating systems.

4. PROCEDURES.

a. General Procedures.

(1) The DJS network shall be protected by a firewall which is managed by a Firewall Administrator and/or an alternate administrator designated by the Chief Information Officer (CIO). The firewall will produce log files which shall be stored in a secured location and backed up onto tape. These tapes shall be taken off-site bi-weekly for storage. Reports shall be generated and made available to the DJS Data Security Officer for daily reviews.

(2) The DJS firewall shall be configured to block all unused ports, limit administrative access to IP address' or subnets assigned to administrators of the firewall device, maintain comprehensive audit trails, and ensure publicly accessed servers are protected against intrusion and attacks by configuring a separate network interface which will be designated as a Demilitarized Zone (DMZ).

(3) The DJS network shall have an extra layer of protection through the use of an Intrusion Detection/Prevention (IDP) protection device.

b. Firewall Administrator's Responsibilities.

(1) Ensure the firewall logs are available to be reviewed. The firewall will produce a log file which will track all activities of the firewall. Through the use of third-party software, the logs will generate various reports which will be reviewed daily by the Data Security Officer and/or alternate.

(2) Investigate all firewall anomalies and determine the escalation priority. When anomalies are identified by the DJS Data Security Officer and/or designee, the Firewall Administrator will be notified. The Firewall Administrator will investigate the anomaly and determine how to proceed with addressing the issue.

(3) Update the firewall operating system. The administrator is responsible for keeping the firewall operating system patched with the applicable updates available which will address newly identified vulnerabilities.

(4) Store all log files off-site to removable media on a bi-weekly basis. Log files will be backed up onto tape and stored bi-weekly off-site. This backup job will be configured as part of the backup cycle.

(5) Submit reports as requested by DJS Executive Staff and approved by the DJS CIO. Periodically, reports are requested to track certain activities of the firewall. The administrator is responsible for creating the reports as

requested and approved. These requests must be submitted in writing and signed off by the CIO and requestor.

c. Configuration Change Procedures.

(1) The Firewall Administrator shall make all changes to the firewall as necessary.

(2) All changes and testing must be submitted to the CIO as a project plan. The approved project plan will serve as the log of changes and stored on the server with the log files. In the case of an emergency, approval and a project plan is not required at the time of the emergency, however, a completed emergency project plan shall document all changes made and shall be completed within five working days of the emergency and submitted to the CIO.

d. DJS Data Security Officer Responsibilities.

The firewall reports generated from the log files will be reviewed daily by the Data Security Officer and/or alternate for anomalies. Anomalies are reported to the Firewall Administrator and/or alternate to be investigated. Daily findings and a summary of report reviews will be reported as a Firewall Status Report. This report will be submitted to the Firewall Administrator to be stored in a secured folder on a server for future reference.

5. DIRECTIVES/POLICIES AFFECTED.

a. Directives/Policies Rescinded - **None.**

b. Directives Referenced - **None.**

6. LOCAL IMPLEMENTING PROCEDURES REQUIRED. Yes.

7. FAILURE TO COMPLY.

Failure to comply with a Secretary's Policy and Procedure shall be grounds for disciplinary action up to and including termination of employment.

Appendix – None.

MARYLAND DEPARTMENT OF JUVENILE SERVICES
EMPLOYEE STATEMENT OF RECEIPT
POLICY AND PROCEDURE

SUBJECT: Firewall Security Policy
POLICY NUMBER: IT-01-08 (Information Technology)
EFFECTIVE DATE: June 6, 2008

I have received one copy (electronic or paper) of the Policy and/or Procedure as titled above. I acknowledge that I have read and understand the document, and agree to comply with it.

_____ _____
SIGNATURE PRINTED NAME

_____
DATE

(THE ORIGINAL COPY MUST BE RETURNED TO YOUR IMMEDIATE SUPERVISOR FOR FILING WITH PERSONNEL, AS APPROPRIATE.)